(12) UK Patent Application (19) GB (11) 2 264 373 (13) A

(43) Date of A publication 25.08.1993

(21) Application No 9202451.2

(22) Date of filing 05.02.1992

(51) INT CL[5]
G06F 12/14

(52) UK CL (Edition L)
G4A AAP

(56) Documents cited
None

(58) Field of search
UK CL (Edition K) G4A AAP
INT CL[5] G06F 12/14

(71) Applicant
Eurologic Research Limited

(Incorporated in Ireland)

49 Bracken Road, Sandyford Industrial Estate,
Dublin 18, Ireland

(72) Inventor
Mark Nolan

(74) Agent and/or Address for Service
Haseltine Lake & Co
Hazlitt House, 28 Southampton Buildings,
Chancery Lane, London, WC2A 1AT, United Kingdom

(54) Data encryption

(57) An apparatus 10 for encrypting data to be stored on a tape 11 or other storage medium includes means 20 to encrypt different blocks of data using respective different keys which are derived from a common key as a function of the storage location of the data.

The different keys may alternatively be derived from the common key as a function of the position of a filename in an index or the quantity of data to be stored.

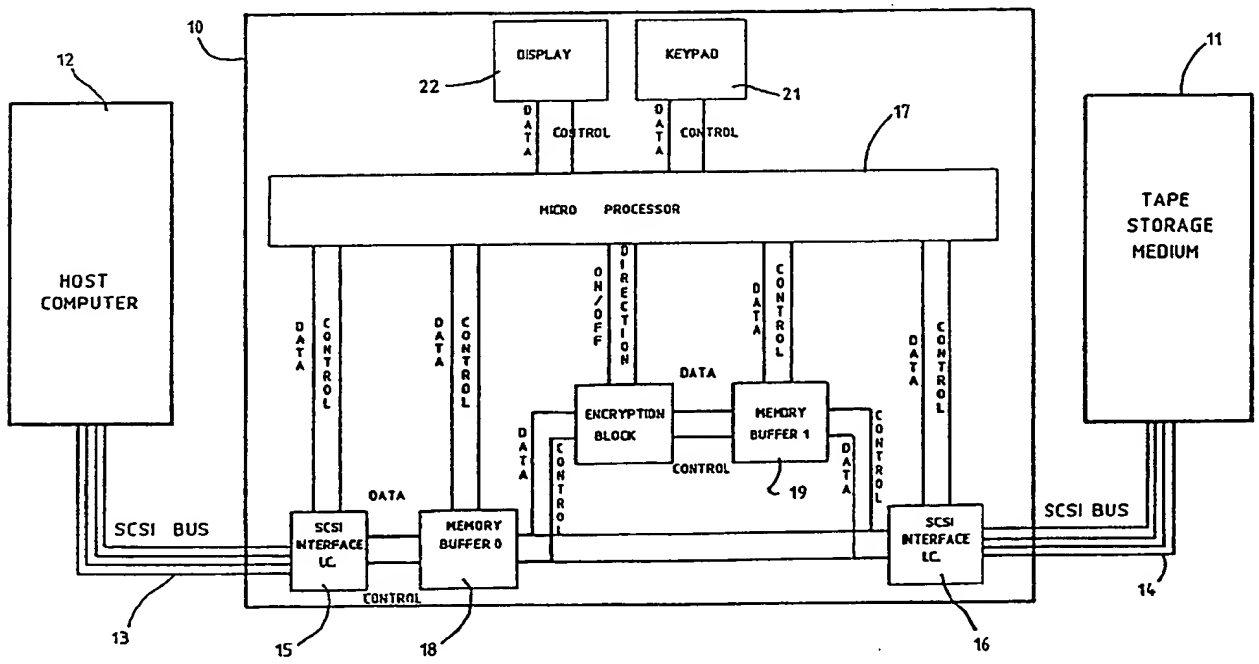

FIG 1

GB 2 264 373 A

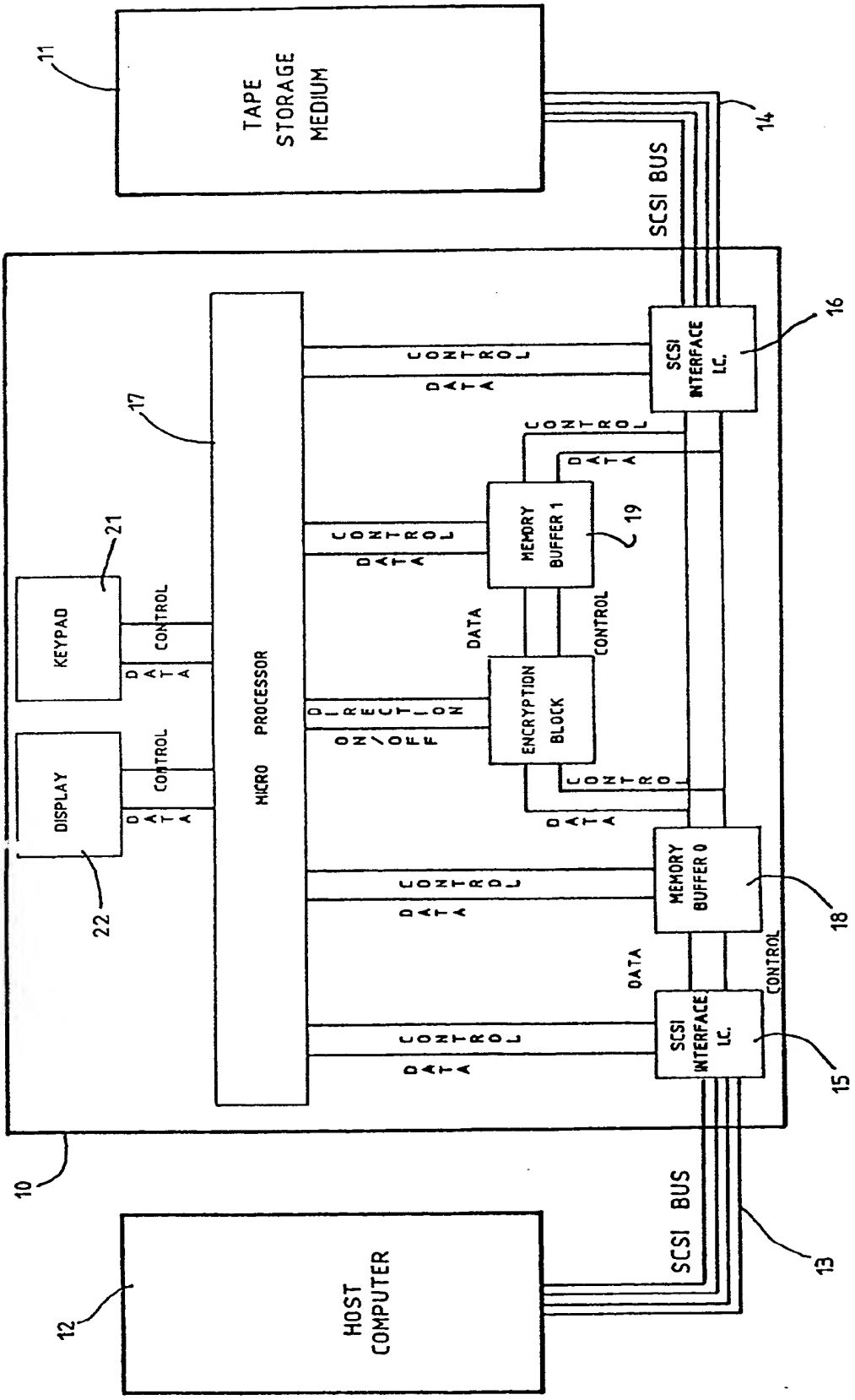

FIG 1

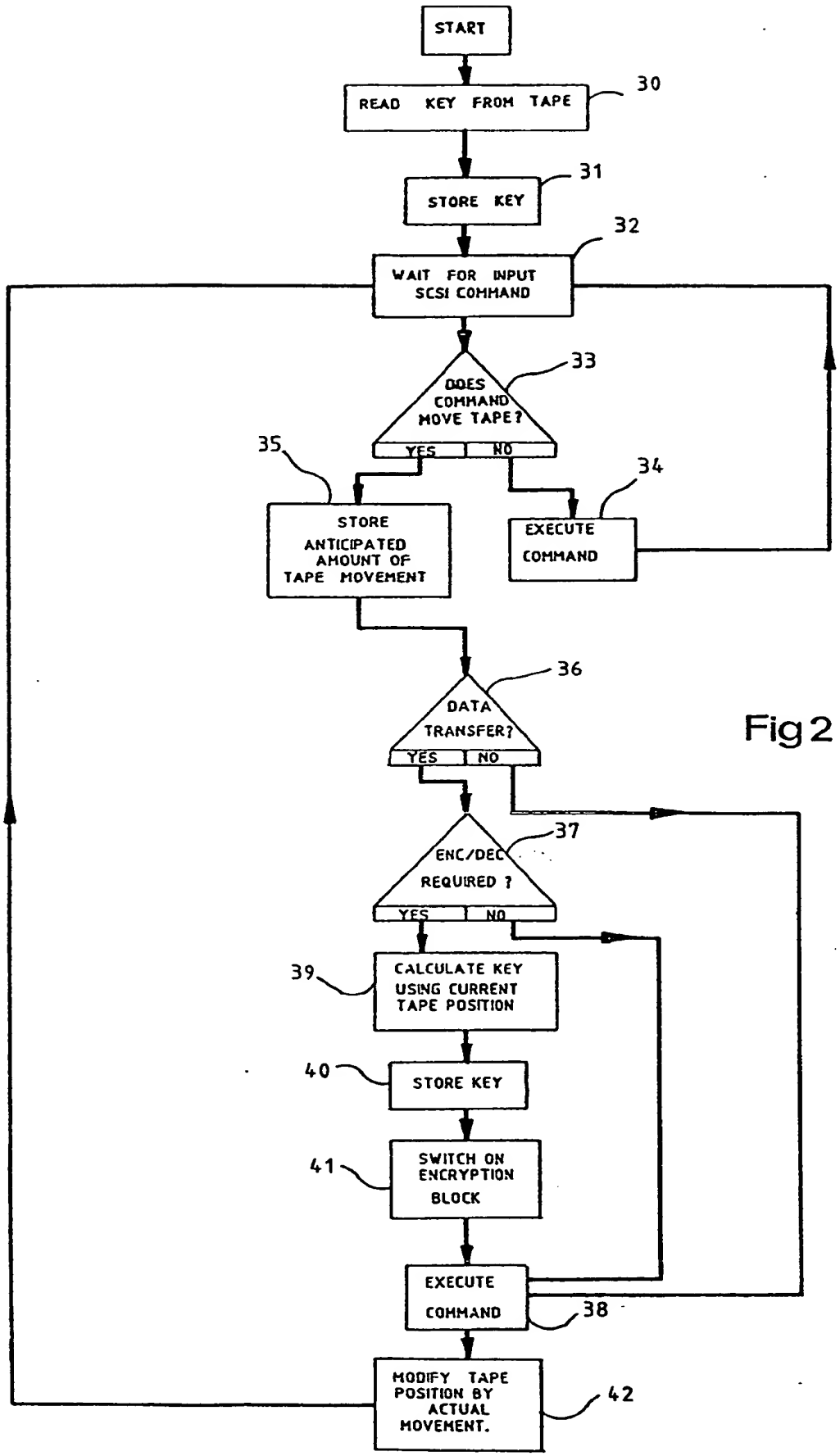

Fig 2

DATA ENCRYPTION APPARATUS AND METHOD

This patent relates to an apparatus and method for the encryption of computer data before storage.

Modern encryption algorithms use a number called a key. Each key uniquely defines the way data is to be encrypted.

One way of deciphering encrypted data without knowing the key is to compare known plain data with the same data when encrypted. In this way a translation table for all values of input data, and the corresponding encrypted data, can be built up. To prevent this it is recommended that a new key is used each time a block of data is encrypted.

For added security it is also recommended that the way in which data is encrypted is a function of the data itself as well as of the key. A unit of input data is encrypted and the result is fed back to modify how the next unit is to be encrypted. This mode of operation is known as 'Cipher Feedback'.

To achieve these two objectives on a tape drive a random key would normally be generated, encrypted using a fixed key and stored with each block of data on the tape. A 'block' of data may consist of either all the data stored on a tape or some smaller subdivision. This method has disadvantages however.

Because of cipher feedback each unit of output encrypted data is a function of the data which precedes it. If the data block chosen is the entire tape then in order to read from a particular location on the tape all data which precedes that tape position must be decrypted. This slows down the read operation considerably.

If the data block chosen is some smaller subdivision of the tape contents then a new key must be stored with each block of data on the tape. This reduces the amount of plain data that can be stored. Furthermore when a number of blocks are to be read from the tape the key must be read and changed for each block required. This also slows down the read operation considerably. The structure of the data on the tape is also considerably different from that intended by the host computer adding considerably to the computational overhead required to keep requested operations compatible with those executed by the tape drive.

It is therefore the object of the invention to provide an apparatus and method which can subdivide the data stored on tape or other storage medium into blocks each of which are uniquely encrypted, without storing a separate key for each block.

Accordingly, the present invention provides a method of encrypting data to be stored on a storage medium, wherein different blocks of data are encrypted using respective different keys which are derived from a common key as a function of the storage location of the data.

The invention further provides an apparatus for encrypting data to be stored on a storage medium, including means to encrypt different blocks of data using respective different keys which are derived from a common key as a function of the storage location of the data.

The embodiment of the invention to be described, which relates to the storage of data on tape, uses a single key on each tape of data, common to all the data. The particular key used to encrypt or decrypt a given data block is then produced by modifying the common key by a number which corresponds with the location on the tape, as reported by the tape drive, which may or may not correspond to a physical location on the tape, at which the data is to be stored. The tape position is measured in terms of 'Filemarks' and 'Save Set Marks' although it is recognised that many other units could be used. All the data from a filemark, save set mark or the beginning of tape up to the subsequent filemark or save set mark are treated as a block of data for the purpose of encryption.

A 'Filemark' is a special recorded element, containing no user data, which is stored on the tape to separate logical groupings of data from each other.

A 'Save Set Mark' is also a special recorded element containing no user data, which provides a segmentation scheme hierarchically superior to a filemark.

The embodiment of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of an apparatus for encryption of data according to the embodiment of the invention; and

Figure 2 is a flow diagram of the main program steps performed by the microprocessor in Figure 1.

The embodiment is designed for use with tape drives which use the so-called 'Small Computer System Interface' (SCSI). Normally a tape drive 11 is directly connected to a host computer 12 via a SCSI cable (SCSI bus). When the encryption/decryption apparatus 10 according to the embodiment of the invention is installed, two SCSI cables are used - one cable 13 which connects to the host computer 12 and a second cable 14 which connects to the tape drive 11. In this way all data transferred to or from the tape drive passes through the apparatus 10 and can be encrypted or decrypted as required.

The apparatus 10 has on each side a respective interface 15, 16 to the SCSI bus 13, 14 respectively. The host computer interface 15 can, under the control of a microprocessor 17, transfer data directly to or from

a host memory buffer 18. The target tape drive interface 16 can, under the control of the microprocessor 17, transfer data to or from the host memory buffer 18 or a target memory buffer 19. There is also an encryption block 20, and this can also transfer data to or from the host memory buffer 18 and the target memory buffer 19, under the control of the microprocessor 17.

The host computer interface 15, the tape drive interface 16 and the encryption block 20 access the memory buffers 18 and 19 using a request signal. This signal indicates to a memory block that a byte of data is ready to be read or written. Whether a particular memory block responds to that request is controlled by the microprocessor 17. The microprocessor can, in this way, switch on and off the flow of data into and out of a particular memory buffer from a particular source or destination. It also determines the address in the memory buffer at which the data is to be stored.

If encryption or decryption is not required both interfaces 15 and 16 transfer data to and from the host memory buffer 18.

If decryption or encryption is required the host and target interfaces 15 and 16 transfer data to or from their respective memory buffers 18 and 19. The microprocessor 17 passes the encryption key to the encryption block 20 and sets it to either encrypt or decrypt. The data is then transferred through the encryption block 20 from one of the memory buffers 18, 19 into the other, according to the direction of data

flow, i.e. according to whether data is being encrypted or decrypted. The encryption block 20 may operate to encrypt/decrypt the data according to any desired encryption algorithm, such as the DES algorithm.

A keypad 21 is used to configure the operation of the apparatus 10 and to select the single encryption key for a tape. This key, which is to be common to all the data on the tape, is stored on the tape before any data is written to the tape. A display 22 is used to show status and error information and the current configuration.

Figure 2 is a flow diagram showing the main steps of the program controlling the microprocessor 17.

After initialisation 30, 31, during which the microprocessor 17 reads the common encryption key stored on the tape and stores it in the unit 10, the microprocessor 17 waits for a command tc be sent from the host computer, step 32. It then establishes whether or not the command involves any movement of the tape, step 33. If not, the command is executed, step 34, and the microprocessor waits for further commands. If it does involve tape movement, the anticipated amount of movement is calculated and stored, step 35. The microprocessor then ascertains whether any transfer of encrypted data is required, steps 36 and 37. If not, the command is executed, step 38. If it does involve the transfer of encrypted data then the stored encryption key is modified by the current tape position, step 39. The new encryption key is then passed to the encryption block, step 40, and the encryption block is

set to encrypt or decrypt, step 41. The required command is then executed at step 38. The stored tape position is then modified by the actual tape movement which has occurred, step 42. This movement may differ from that anticipated when a command is initiated. The end of tape may, for example, be reached. If such an error does occur the actual amount of tape movement can be calculated from information received from the tape drive.

As previously stated the tape position is measured in terms of filemarks and save set marks. A count is kept of the number of save set marks which exist between the start of the tape and the actual tape position. The filemarks are counted from the previous save set mark, or from the beginning of the tape if no save set marks exist, up to the actual tape position. The filemark counter is reset, therefore, after each save set mark.

The key is changed after each filemark or save set mark. The key used is as follows:

New key =
Common key for tape + Set_count * 1000000h + File_count

where 'Set_count' is the save set mark counter and 'File_count' is the filemark counter as described above. All data up to the next filemark or save set mark is encrypted using this key.

Various modifications are possible within the scope of the invention. For example, the invention can be used for other storage media such as disk drives,

optical disk drives, optical tape drives, random access memory, read only memories, paper tape, magnetic core memory, bubble memory, punch cards, medium changers and others yet to be developed.

Also, other methods can be used to establish the storage location of data, as reported by the storage device, such as beginning of medium, end of medium, addresses, tape partitions, disk partitions, disk sectors, tape tracks, data frames, storage block number, files, file descriptor blocks, end of data marker, file number, etc.

It is further recognised that instead of using the position of the data to modify the common key for each data block, the position of a filename in an index could be used to modify the common encryption key for each block, or the quantity of data in the block could be used to modify the common key.

Further, the invention can be used to encrypt and decrypt data on two ends of a bus, for example a SCSI bus, to protect the bus itself.

It is further recognised that the invention could be used in relation to other interfaces such as ST506, ESDI, SMD, FI, PERTEK, STC, QIC-02, proprietary interfaces and others yet to be developed and to use command protocols other than SCSI-1 and SCSI-2.

The invention is not limited to the embodiments described herein which may be modified or varied without departing from the scope of the invention.

CLAIMS:

1. An apparatus for encrypting data to be stored on a storage medium, including means to encrypt different blocks of data using respective different keys which are derived from a common key as a function of the storage location of the data.

2. An apparatus as claimed in Claim 1, wherein the storage medium is a tape.

3. An apparatus as claimed in Claim 2, wherein the common key is common to all the data on the tape and is stored on the tape.

4. An apparatus as claimed in Claim 3, wherein the storage location of the data is measured in terms of filemarks and save set marks.

5. An apparatus as claimed in Claim 4, wherein a block of data comprises all the data from a filemark, save set mark or the beginning of tape up to the subsequent filemark or save set mark.

6. An apparatus as claimed in Claim 5 wherein the key for a particular block of data is derived according to the following formula:

Key for block =
Common key for tape + Set_count * 1000000h + file count.

7. A method of encrypting data to be stored on a storage medium wherein different blocks of data are encrypted using respective different keys which are derived from a common key as a function of the storage location of the data.

8. An apparatus for encrypting data to be stored on a storage medium, including means to encrypt different blocks of data using respective different keys which are derived from a common key as a function of the position of a filename in an index or of the quantity of data stored.

9. A method of encrypting data to be stored on a storage medium wherein different blocks of data are encrypted using respective different keys which are derived from a common key as a function of the position of a filename in an index or of the quantity of data stored.

10. An apparatus for encrypting data substantially as described with reference to the accompanying drawings.

11. A method for encrypting data substantially as described with reference to the accompanying drawings.

Amendments to the claims have been filed as follows

7. A method of encrypting data to be stored on a storage medium wherein different blocks of data are encrypted using respective different keys which are derived from a common key as a function of the storage location of the data.

8. An apparatus for encrypting data substantially as described with reference to the accompanying drawings.

9. A method for encrypting data substantially as described with reference to the accompanying drawings.

12.

Patents Act 1977
Examiner's report to the Comptroller under Section 17 (The Search Report)

Application number
9202451.2

Relevant Technical fields

(i) UK Cl (Edition K) G4A (AAP)

(ii) Int CL (Edition 5) G06F 12/14

Search Examiner
S J PROBERT

Databases (see over)

(i) UK Patent Office

(ii) ONLINE DATABASE: WPI

Date of Search
15 APRIL 1992

Documents considered relevant following a search in respect of claims 1-7

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
	NONE	

SF2(p)

lme - c:\wp51\doc99\fil000677

Category	Identity of document and relevant passages	Relevant to claim(s)

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).

93 at The Patent Office, Concept House, Cardiff Road, Newport, Gwent NP9 1RH. Further copies may be obtained from t 6, Nine Mile Point, Cwmfelinfach, Cross Keys, Newport, NP1 7HZ. Printed by Multiplex techniques ltd, St Mary Cray, Kent.